DETAILED ACTION

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Jamie Ross on October 22, 2009.

The application has been amended as follows:

IN THE SPECIFICATION:

Please amend the paragraph spanning Page 15, line 13-Page 16, line 12 as follows:

The computer on which the SPAM reporting system is installed may be a stand-alone desktop computer, laptop computer, server, mainframe, or a mobile or handheld computing device (e.g., personal digital assistant (PDA) or mobile phone), for example. Fig. 3 shows a system block diagram of computer system 60 that may be used as the user computer, server, or other computer system to execute software of an embodiment of the invention. As shown in Fig. 3, the computer system 60 includes memory 62 which can be utilized to store and retrieve software programs incorporating computer code that implements aspects of the invention, data for use with the invention, and the like.

Exemplary computer readable storage media include CD-ROM, floppy disk, tape, flash memory, system memory, and hard drive. ~~Additionally, a data signal embodied in a carrier wave (e.g., in a network including the Internet) may be the computer readable storage medium.~~ Computer system 60 further includes subsystems such as a central processor 64, fixed storage 66 (e.g., hard drive), removable storage 68 (e.g., CD-ROM drive), and one or more network interfaces 70. Other computer systems suitable for use with the invention may include additional or fewer subsystems. For example, computer system 60 may include more than one processor 64 (i.e., a multi-processor system) or a cache memory. The computer system 60 may also include a display, keyboard, and mouse (not shown) for use as a desktop or laptop computer.

IN THE CLAIMS:

Claim 1: A method for generating a report on an unsolicited electronic message, comprising: receiving an electronic mail message; determining whether the electronic message is an unsolicited message; if the message is an unsolicited message, examining the message to identify a network address relating to the message, identifying an authority hosting the network address, generating a report containing the identified network address and hosting authority, and transmitting the report to a central managed service provider, where the central managed service provider collects threat information from one or more organizations and reports to the hosting authority once a predetermined amount of threat information has been collected; wherein identifying the

hosting authority comprises identifying an owner of a network domain; wherein reporting to the hosting authority includes the central managed service provider transmitting a hosting authority message including the collected threat information to the hosting authority; wherein the hosting authority message that the central managed service provider transmits to the hosting authority includes a hosting authority report that includes a content of the message, a date and time the message arrived on a recipient's server, an IP address and name reported during an SMTP connection associated with the message, and a full WHOIS report used to track down the hosting authority.

Claim 13: A system, the system comprising: a detector that detects a network address within an electronic message identified as an unsolicited message; a host identifier that identifies an authority hosting the network address; a report generator that generates a report containing the identified network address and hosting authority; and a tangible computer readable storage medium that at least temporarily stores the identified network address and hosting authority; wherein identifying the hosting authority comprises identifying an owner of a network domain; wherein the system is operable such that the report is transmitted to a central managed service provider, where the central managed service provider collects threat information from one or more organizations and reports to the hosting authority once a predetermined amount of threat information has been collected; wherein reporting to the hosting authority includes the central managed service provider transmitting a hosting authority message including the collected threat information to the hosting authority; wherein the system is

operable such that the hosting authority message that the central managed service provider transmits to the hosting authority includes a hosting authority report that includes a content of the message, a date and time the message arrived on a recipient's server, an IP address and name reported during an SMTP connection associated with the message, and a full WHOIS report used to track down the hosting authority.

Claim 22: A computer product embodied on a tangible computer readable storage medium, comprising: code that receives an electronic mail message; code that determines whether the electronic message is an unsolicited message; code that examines the message to identify a network address relating to the message if the message is an unsolicited message; code that identifies an authority hosting the network address; code that generates a report containing the identified network address; and a computer readable medium that stores said computer codes; wherein identifying the hosting authority comprises identifying an owner of a network domain; wherein the computer product is operable such that the report is transmitted to a central managed service provider, where the central managed service provider collects threat information from one or more organizations and reports to the hosting authority once a predetermined amount of threat information has been collected; wherein reporting to the hosting authority includes the central managed service provider transmitting a hosting authority message including the collected threat information to the hosting authority; wherein the computer program product is operable such that the hosting authority message that the central managed service provider transmits to the hosting authority

includes a hosting authority report that includes a content of the message, a date and time the message arrived on a recipient's server, an IP address and name reported during an SMTP connection associated with the message, and a full WHOIS report used to track down the hosting authority.

Claim 32: Cancelled.

Reasons for Allowance

2. Claims 1-8, 10-31 & 33 are allowed.

3. The following is an examiner's statement for reasons for allowance: The prior art of record Aronson et al (U.S. 6,654,787 B1), Hall (U.S. 6,915,334 B1) and Leeds (U.S. 6,393,465 B2) fails to teach the invention as claimed. For instance prior art was not found to teach "A method for generating a report on an unsolicited electronic message, comprising: receiving an electronic mail message; determining whether the electronic message is an unsolicited message; if the message is an unsolicited message, examining the message to identify a network address relating to the message, identifying an authority hosting the network address, generating a report containing the identified network address and hosting authority, and transmitting the report to a central managed service provider, where the central managed service provider collects threat information from one or more organizations and reports to the hosting authority once a predetermined amount of threat information has been collected; wherein identifying the

hosting authority comprises identifying an owner of a network domain; wherein reporting to the hosting authority includes the central managed service provider transmitting a hosting authority message including the collected threat information to the hosting authority; wherein the hosting authority message that the central managed service provider transmits to the hosting authority includes a hosting authority report that includes a content of the message, a date and time the message arrived on a recipient's server, an IP address and name reported during an SMTP connection associated with the message, and a full WHOIS report used to track down the hosting authority."

4. Dependent claims further limit the independent claims and are considered allowable on the same basis as the independent claims as well as for further limitations set forth. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance".

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ASGHAR BILGRAMI whose telephone number is (571)272-3907. The examiner can normally be reached on 9-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tonia L.M. Dollinger can be reached on 571-272-4170. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/A. B./
Examiner, Art Unit 2443

/George C Neurauter, Jr./
Primary Examiner, Art Unit 2443